Fast Flux Service Networks: Dynamics and Roles in Hosting Online Scams*

Maria Konte, Nick Feamster
Georgia Tech
{mkonte, feamster}@cc.gatech.edu

Jaeyeon Jung
Intel Research
jaeyeon.jung@intel.com

ABSTRACT

This paper studies the dynamics of fast flux service networks and their role in online scam hosting infrastructures. By monitoring changes in DNS records of over 350 distinct fast flux domains collected from URLs in 115,000 spam emails at a large spam sinkhole, we measure the rate of change of DNS records, accumulation of new distinct IPs in the hosting infrastructure, and location of change both for individual domains and across 21 different scam campaigns.

We find that fast flux networks redirect clients at much different rates—and at different locations in the DNS hierarchy—than conventional load-balanced Web sites. We also find that the IP addresses in the fast flux infrastructure itself change rapidly, and that this infrastructure is shared extensively across scam campaigns, and some of these IP addresses are also used to send spam. Finally, we compared IP addresses in fast-flux infrastructure and flux domains with various blacklists (i.e., SBL, XBL/PBL, and URIBL) and found that nearly one-third of scam sites were not listed in the URL blacklist at the time they were hosting scams. We also observed many hosting sites and nameservers that were listed in both the SBL and XBL both before and after we observed fast-flux activity; these observations lend insight into both the responsiveness of existing blacklists and the life cycles of fast-flux nodes.

1. INTRODUCTION

Online scams require victims to contact a point-of-sale Web site, which must be both highly available and dynamic enough to evade detection and blocking. Until recently, many sites for a scam were hosted by a single IP address for a considerable amount of time (i.e., up to a week) [2]; unfortunately, the relatively static nature of these sites made it possible to block scams with simple countermeasures, such as blocking the IP address. To maintain sites that are both dynamic and highly available, cybercriminals are increasingly using *fast flux*—a DNS-based technique used by botnets to rapidly change these delivery sites.

In this paper, we find that the scam infrastructure has become considerably more sophisticated and dynamic. Indeed, in this paper we show that attackers have developed a sophisticated infrastructure for directing victims to scam sites that move around frequently to evade detection and blocking. Attackers that mount scam campaigns appear to be making extensive use of fast-flux service networks [8], which can dynamically (and quickly) redirect clients to different sites for hosting scams. The machines that host content are typically ephemeral (i.e., they may simply be compromised machines) and distinct from the controllers that provide content and control redirections.

This paper studies the dynamics of fast-flux service networks as they are used to host point-of-sale sites for email scam campaigns. We study the scam sites that were hosted by more than 350 domains as part of 21 scam campaigns in over 115,000 emails collected over the course of a month at a large spam simkhole. We study characteristics of *dynamics* of the infrastructure hosting fast-flux service networks, the *roles* that various machines play in hosting online scams, and the effectiveness of various blacklists at identifying IP addresses and URLs of scam sites.

Previous work has studied the rates at which fast-flux networks change DNS A-record mappings (i.e., name to IP address mappings) and the rate at which new IP addresses are accumulated [6]; this paper expands on that study and presents many new classes of findings. First, we study fast-flux networks *by campaign* to determine whether dynamics differ across campaigns, and whether distinct spam campaigns share fast-flux service infrastructure. Second, we perform continual and iterative DNS monitoring to discover the locations in the DNS hierarchy where fast-flux networks dynamically redirect clients. Finally, we study the roles of fast-flux nodes in hosting different parts of the infrastructure (e.g., authoritative name server, Web server, or spammer) and how these roles evolve over time.

Table 1 summarizes the findings of our study and possible implications for these findings. We present findings regarding the following aspects of fast-flux networks:

- *Rate of change.* We examine the rates at which fast-flux networks redirect clients to different authoritative name servers (either by changing the authoritative nameserver's name or IP address), or to different Web sites entirely. We find that, while the DNS TTL val-

*The authors will publish their dataset and analysis scripts and would like to be considered for the best paper award.

Finding	Table/Figure	Implications
Dynamics		
Rates of change. DNS records change more quickly than TTL values. NS records are more stable than A records or IPs of NS records. DNS records for fast flux domains change more quickly than those from "legitimate" popular domains.	Fig. 3, Fig. 4	Blacklisting authoritative name server names may help with fast-flux mitigation.
Rates of accumulation. Different scam campaigns (and URLs for those campaigns) recruit new IP addresses at different rates	Fig. 6	The rate at which a URL "accumulates" new IP addresses may help detect fast flux networks and also identify scam campaigns.
Location of change in DNS hierarchy. Different fast-flux domains change at different locations in the DNS hierarchy (i.e., A records, IP of NS record, NS record).	Tab. 6	
Roles		
Sharing. Different scam campaigns share fast-flux infrastructure	Tab. 3, Tab. 4, Tab. 9	Identifying fast-flux *infrastructure* may help with early detection of scam campaigns.
Distribution across /24s. Fast flux domains return A records that are distributed over a far larger set of /24s than legitimate popular Web sites (as seen when queried from a single DNS location).	Fig. 9	The distribution of query results across IP address space may be useful for detecting fast-flux activity.
Distribution in IP address space. A and NS records are distributed across IP address space, but some regions have a high density of both fast-flux agents and spammers.	Fig. 7	Detection of spammers might also help detect fast-flux networks, and vice versa.
Blacklists. Some IP addresses that appear as flux agents appear in spam and exploit blacklists weeks later.	Fig. 10, Tab. 10, Tab. 11	Identification of FF infrastructures can help towards earlier blacklisting of spam/exploit IPs and vice versa.

Table 1: Summary of results.

ues do not differ fundamentally from other sites that do DNS-based load balancing, the rates of change (1) differ fundamentally from legitimate load balancing activities; (2) differ across individual scam campaigns.

- *Rate of accumulation ("recruit").* We study the extent to which individual fast-flux networks "recruit" new IP addresses and how the rate of growth varies across different scam campaigns. We find that, while there is a considerable amount of sharing of IP addresses across different scam campaigns, different campaigns accumulate new IP addresses at different rates.
- *Location of change.* We study the extent to which fast-flux networks change the Web servers to which clients are redirected. We infer the location of change by monitoring any changes of (1) the authoritative nameservers for the domains that clients resolve (the NS record, or the IP address associated with an NS record) or of (2) the mapping of the domain name to the IP address itself (the A record for the name). We find that behavior differs by campaign, but that many scam campaigns redirect clients by changing *all* three types of mappings, whereas most legitimate load-balancing activities only involve changes to A records.
- *Use and sharing of infrastrcture.* We study the geographical and topological locations of fast-flux hosts (both authoritative nameservers and Web servers), as well as how fast-flux infrastructure is shared over time, across scam campaigns, and between spamming and hosting infrastructure. We find that different scam campaigns share fast-flux infrastructure; we also find overlap between spamming infrastructure and online scam hosting infrastructure.

Our findings lend insights into the operation of fast-flux networks that may ultimately lead to more effective mitigation techniques: Although scam campaigns are short-lived, the infrastructure that hosts these scams (i.e., the fast-flux network or networks) appears to have relatively invariant features that may prove useful for identifying scams and the spam messages that advertise them.

The rest of this paper is organized as follows. Section 2 describes background on fast-flux networks, current understanding about their roles in hosting online scams, and related work in studying fast-flux networks. Section 3 describes our data collection methods, as well as various limitations of our dataset. Section 4 describes the dynamics of fast-flux service networks that we observed hosting 21 different spam campaigns over the course of a month. Section 5 describes the roles that we observed each IP address playing in the fast flux networks, the locations of spammers and fast flux infrastructure in the IP address space, and the sharing of infrastructure across different roles. Section 6 describes the relationships between when various blacklists listed IP addresses and when these IP addresses were seen in the fast-flux hosting infrastructure that we observed in our data. Section 7 concludes with a summary and discussion of future work.

2. BACKGROUND AND RELATED WORK

We describe main redirection techniques commonly employed by fast flux service networks and show an example illustrating how this technique can be observed from DNS responses. We then discuss related work.

2.1 Fast-Flux Mechanics

Domain name: pathsouth.com & responding authoritative nameserver: 218.236.53.11

Spam sent by IPs	Time: 20:51:52 (GMT) A records	TTL	NS records	TTL	IP addresses of NS records	TTL
88.234.185.68, 88.229.212.225, 212.156.205.188, 189.4.136.197, 89.132.220.6, 125.27.211.201, 85.109.43.187, 83.27.32.75, 80.94.175.76, 84.115.175.16, 88.65.174.73, 195.8.27.96, 124.28.82.112	77.178.224.156, 79.120.37.38, 79.120.63.225, 79.120.72.0, 79.120.101.244, 79.120.107.25, 85.216.198.225, 87.228.106.92, 89.20.146.249, 89.20.159.226, 89.176.63.78, 89.208.2.199, 89.208.5.106, 213.141.146.83, 220.208.7.115	300	ns0.nameedns.com, ns0.nameedns1.com, ns0.renewwdns.com, ns0.renewwdns1.com	172800	218.236.53.11, 89.29.35.218, 78.107.123.140, 79.120.86.168	172800
	Time: 20:57:49 (GMT) A records	TTL	NS records	TTL	IP addresses of NS records	TTL
	61.105.185.90, 69.228.33.128, 79.120.37.38, 79.120.108.136, 85.216.198.225, 87.228.106.92, 89.20.146.249, **89.20.159.178**, **89.29.35.218**, **91.122.121.88**, **213.220.251.97**, **218.254.157.62,** **218.255.10.103,** 220.208.7.115, **222.5.114.183**	300	ns0.nameedns.com, ns0.nameedns1.com, ns0.renewwdns.com, ns0.renewwdns1.com	172800	218.236.53.11, 89.29.35.218, 78.107.123.140, **213.248.28.235**	172800

Table 2: DNS lookup results of the `pathsouth.com` fluxing domain: The IP addresses in bold highlight changes between the two lookups six minutes apart.

Fast flux is a DNS-based method that cybercriminals use in order to organise, sustain and protect their service infrastructures such as illegal web hosting and spamming [21]. Multiple cybercriminal families have been observed to use the fast flux techniques for illegal or fake online businesses, phishing sites, adult content sites [14]. Somewhat similar to a technique used by content distribution networks (CDNs) such as Akamai, a fast-flux domain is served by many distributed machines and short time-to-live (TTL) values are used to quickly change a mapping between a domain and an IP address. However, the hosts involved for serving a fast-flux domain are botnet zombie drones and instead of hosting actual content, these zombies often act as front-end proxies that relay messages between a client and a "mothership" node [21]. Consequently, using this fast flux technique, cybercriminals can easily throw in and out a large number of compromised hosts as needed while effectively hiding their mothership node.

Variations of the technique also exist [21]. In addition to fluctuating address records (A records), a fast-flux domain can have changing name servers records (NS records or IP addresses of NS records). In practice, any combinations of DNS record fluctuations can be used for flexible and resilient operations. Moreover, as we will show in Section 4.3, many hosts exploited by fast-flux service networks are found to play the role of both a hosting server (or a front end proxy of it) and an authoritative name server (or a front end proxy of it).

The dynamics of fast-flux service networks make ineffective the existing mitigation scheme that relies on blacklisting offending hosts. Operators of such networks can simply swap out blacklisted hosts. Moreover, by constantly monitoring the "health" of individual hosts, the operators can increase service availability from likely unstable compromised machines. To demonstrate how quickly fast-flux service networks change, we show an example of a fast-flux domain that we monitored on January 20, 2008 at 20:51:52 GMT. The fast-flux domain is called `pathsouth.com` and at that time it was pointing to one of illegal pharmaceutical companies called Canadian Pharmacy [18]. Table 2 shows the DNS records resulted from two lookups with seven minutes apart. The first column shows the IP addresses of spam sources, from which our spamtrap received copies of spam containing the fast-flux domain. The ten records in bold show that the domain swapped in nine new hosts for serving content and one new name server.

2.2 Related Work

The operation of fast-flux service networks was first described in detail by the Honeynet Project [21]. By closely monitoring the behavior of fast-flux agents executed in test environments, the report showed two different types of fast-flux service networks—single-flux and double-flux. Their findings provide insights on the changing nature of fast-flux service networks and lead us to design the multi-level measurement method that form the bases of our study of dynamics of scam infrastructure.

Because it is only less than a year since the details were publicly known, there are few empirical studies on fast-flux networks. Holz *et al.* [6] analyzed fast flux domains using periodic DNS lookups and presented the characteristics focusing on the diversity of A records and the network locations (AS numbers) that these A records reside at. They also showed various analysis results including the percentage of scam campaigns leveraging fast-flux service networks and the rate at which new machines are added to fast flux domains for a few selected ones. In addition to these measurements, we measured the change of fast flux domains at

multiple levels of the DNS hierarchy (A records, NS records, and IPs of NS records) and found many different structures of fast-flux service networks, some of which are previously unknown. We also present the geographic and topological distribution of flux hosts, the prevalence resource sharing found across different scam campaigns, and the relationship between fast-flux agents and various blacklists.

Previous work observed fast-flux domains via DNS measurement [24]. From the analysis of passively collected DNS responses at a university gateway, Zdrnja *et al.* observed an instance of fast-flux domain that was short lived (only for three days) and resolved to 80 different IP addresses [24]. In comparison, our study *actively* probes a large number of suspicious DNS domains to profile different types of fast-flux networks over a longer period of time.

Our primary data is drawn from emails collected at a spam trap. Spam traps provide a window to glimpse into the underlying network operations of online scammers who use bulk email for solicitation. Because of relatively easy deployment and data processing, many previous studies used email collected at spam traps for measuring the effectiveness of DNS-based blacklists [10], studying the network-level behavior of spammers [13], characterizing the scam hosting infrastructure [2], and studying the dynamism of the IP addresses of spammers [23]. Others have used passive DNS monitoring to study the dynamics of botnets [4, 12], which are now believed to host fast-flux networks.

Content-based scam campaign clustering is a commonly used technique for analyzing spammer behavior. Anderson *et al.* used image fingerprints to group similar Web pages [2] . Holz *et al.* used strings found from HTML documents for grouping [6]. Pathak *et al.* propose that spammers could be clustered into campaigns by looking for relationships across SMTP connections [11]. In comparison, we used image comparison in addition to string matches of the names of embedded files of each URL. Although the similarity metric employed in each work is slightly different, we believe that clustering results would not bear too much difference.

3. DATA

Accordingly, our data collection and processing involves three steps: (1) passive collection of spam data; (2) active DNS monitoring of domains for scams contained in those spam messages; (3) clustering of spam and DNS data by campaign. This section describes our method for collecting spam data and monitoring DNS record changes associated with the associated scam campaigns. We also describe how we monitor the DNS dynamics of popular Web sites to use as a baseline for comparison. We then explain how we postprocess the data to group spam email messages (and the associated DNS data) according to common campaigns. Finally, we discuss potential limitations of our data collection and analysis methods.

3.1 Data Collection

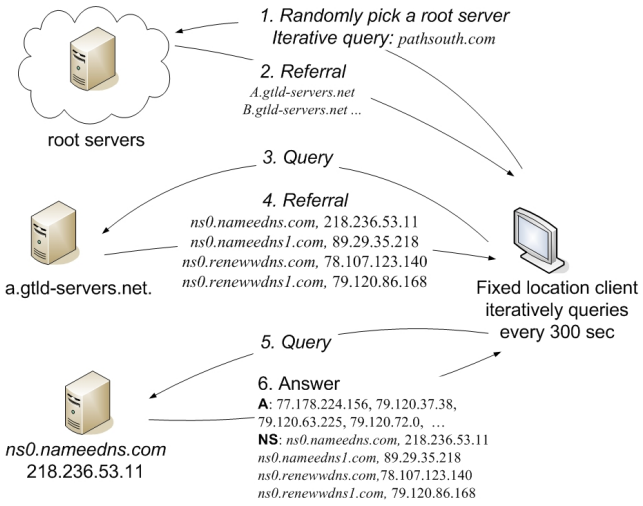


Figure 1: Diagram of the data colletion; a fixed location iterative resolver is set up. The resolver starts the queries from a randomly selected root server, every 300 sec for every domain. Here we feature the same fluxing domain `pathsouth.com` as in Table 2. Our iterative resolver logs all referrals and the DNS records that are returned for every query, at each level of the DNS hierarchy.

To amass a collection of domains to monitor for fast-flux behavior, we collected 3,360 distinct domain names that appeared at spam email messages which were collected at a large spam sink hole. To obtain this list of URLs, we used a simple URL pattern matcher to extract URLs from the bodies of the messages received at the spam trap. We collected these domains over a period of three months, from October 1, 2007 to December 31, 2007.

Next, we implemented an iterative resolver (at a fixed location) to resolve every domain name from this set once every five minutes. Figure 1 shows the method by which our resolver recorded DNS mappings at each level of DNS resolution, which allows us to monitor fast-flux networks for DNS changes at *three distinct locations in the hierarchy*: (1) the A record; (2) the NS record; and (3) the IP addresses corresponding to the names in the NS record. To avoid possible caching effects, the resolver randomly selected a DNS root server at which to start the DNS query. The iterative resolver recorded the answers received at every level of the DNS hierarchy; we recorded all the referrals and the answers by the queried DNS servers for every domain.

Due to the sheer number of DNS lookups required to monitor the domains arriving at the spam trap, the resolver proceeded through the list of domains sequentially: We began by resolving the first 120 domains received at the spam trap each day. Every day the resolver began resolving the next 120 domains on the list. After each domain had been resolved continously for three weeks, we removed the domain from the list. The resolver operated from January 14, 2008

to February 9, 2008.

To compare the dynamics of the domains received at the spam trap as part of online scam campaigns to the DNS dynamics of "legitimate" domains, we used the same iterative resolution process to study the dynamics of the 500 most popular domains, according to Alexa [1].

3.2 Postprocessing: Scam Campaigns

After collecting spam and DNS data, we restricted our analysis to the domains that had reachable Web sites and for which we had observed at least one change in any DNS record. We then clustered the spam messages into *scam campaigns*. To perform this clustering, we retrieve content from the URLs in the email messages and cluster emails whose URLs retrieve common content:

- *Snapshots and Web page sources.* We used AutoIT [3] to sequentially open each URL on a browser, wait until the page is loaded, and take a snapshot of the current page[1]. While doing so, HTTP Analyzer [9] captures all the HTTP requests and responses for further analysis.

- *Clustering by snapshots.* We manually went through snapshot images and cluster URLs if the site is selling the same products under the same brand name using a similar page layout. The clustering is manual and subjective but fairly straightforward.

- *Clustering supplemented with file comparison.* The image comparison fails in the case of partially download pages. For example, `pathsouth.com`, one of the Canadian Pharmacy [18] sites downloads 88 files, of which 85 are jpeg and gif image files. Slow response, which is often observed from fast flux service networks, allows only a few small none image files to be received until the somewhat generous 30 second timeout expires, generating an empty looking page when a snapshot is taken. To make up this shortcoming, for the URLs that are not classified, we check to see whether the downloaded file names of each URL is a subset of those of already identified campaign. We find that most of partially downloaded pages are caused by the Canadian Pharmacy campaign sites and that all of them request `canadian_pharmacy_2_style.css` in common.

Table 3 shows the summary data of 21 campaigns. We denote each campaign with a *category-ID*.[2] The second column is the number of domain names that we found changing during our one month measurement period (fluxing domain). The following two columns show the number of total spam emails containing the fluxing domains that we received at our spam trap and the total number of sender IPs of those spam emails. The last three columns summarize our measurement data: the first two numbers are the total distinct number of IPs returned as A records of domains ($IP_{domains}$) and that of IPs returned as A records of name servers ($IP_{nameservers}$). the last number is the total distinct number of IPs from the combined sets ($IP_{domains} \cup IP_{nameservers}$) . For comparison, Table 4 summarizes the Alexa dataset.

	Domains	IPs of A rec	IPs of NS rec	IPs of A+NS rec
Total	500	1048	852	1877

Table 4: Alexa dataset.

Top campaigns. The top campaign, by the number of hosting servers, is Pharmacy-A. We believe that it is one of Canadian Pharmacy scam campaigns [18]. The campaign swapped in at least of 9,448 distinct IP addresses as hosting servers (or front end proxies of them) for 149 domains over one month. The next two followers are Watch-A [17] and Watch-B [16], both of which offer replica watches. We note that for these top three campaigns, the average ratio of A records associated with a domain name is over 50, allowing the scamsters to freely move around among available hosting servers. However, the remaining campaigns are rather modest and we even see the sharing of a few hosting servers by multiple domains (e.g., Pharmacy-D and Links-B appear to have only 5 hosting servers for 50 and 35 domains respectively). Nonetheless, all 21 campaigns exhibited fluxing behavior in their DNS records to some extent during the measurement period.

Registrars. The fast-flux domains in our dataset are mostly .com (348, or 90.6%). The rest 8.4% are .net (32), .ph (3) and .su (1). However, over 99% of these domains are unique (e.g., a.com, b.com)[3], requiring separate registrations with the corresponding top-level domains. Table 5 shows registrar information of the 384 fast-flux domains that we found on May 7, 2008 via `jwhois` queries. 70% of the domains are still marked as active and registered with eight registrars in China, India, and US. Among these, the three registrars in China are responsible for 257 fast-flux domains (66% of total or 95% of the active ones). Surprisingly, all but `paycenter.com.cn` are ICANN-accredited registrars [7].

Figure 2 shows the month when these domains were registered. Because our data collection was done before February 2008, all the domains were registered before then. Interestingly, however, over 40% were registered in January 2008 and immediately put in use for serving scams. Further, these domains are still active even after four months and the 2% of the domains had been active for over 7 months at the time of our measurement. Unfortunately, our WHOIS lookup is after the fact and thus we are unable to tell whether the 30%

[1]We used a 30 second timeout value to move on to a next URL if the current site is not reachable. The AutoIT script was executed on a virtual machine running Windows XP to avoid possible drive-by infection. We also disabled most security features that display warnings or prompt for approvals as these interfere with automation.

[2]We looked at each Web page snapshot and assigned a category based on offered products.

[3]Only 4 out of 384 fast-flux domains have the same second-level domain name.

Campaign	Spam emails	Spamvertising IPs	Domains in campaigns	Fluxing domains	IPs of A rec	IPs of NS rec	IPs of both A+NS rec
Pharmacy-A	18459	11670	149	149	9448	2340	9705
Watch-A	40681	30411	34	30	1516	225	1572
Watch-B	454	427	43	19	1204	219	1267
Pharmacy-B	371	223	86	52	15	13	22
Casino-A	317	226	6	6	12	12	16
Pharmacy-C	30	4	6	6	12	11	12
Casino-B	15	8	2	1	11	10	17
Links-A	15	8	2	2	10	14	22
Casino-C	4652	4150	9	5	10	14	18
E-Marketing-A	32	4	6	4	8	2	10
Pharmacy-D	37472	28340	52	50	5	5	6
Pharmacy-E	32	25	4	4	5	7	12
Links-B	5663	4573	38	35	5	5	6
Pharmacy-F	2	1	2	2	4	6	10
Pharmacy-G	208	205	2	2	3	8	8
Links-B	4	2	4	2	3	8	11
Service-A	9	1	3	1	2	4	4
Software-A	950	463	5	5	2	4	5
Watch-C	6226	4154	7	5	2	2	2
DomainNames-A	3	3	3	3	2	4	6
Service-B	26	2	2	1	1	3	4
All campaigns	115198	77030	465	384	9521	2421	9821

Table 3: Statistics for fast-flux networks hosting scam campaigns. Campaigns are sorted by the total number of IP addresses returned from A records as the number indicates the size of the underlying infrastructure.

Registrar	Country	Domains
dns.com.cn	China	180 (46.9%)
paycenter.com.cn	China	65 (16.9%)
todaynic.com	China	12 (3.1%)
signdomains.com	India	7 (1.8%)
leadnetworks.com	India	3 (0.8%)
coolhandle.com	US	2 (0.5%)
webair.com	US	1 (0.3%)
stargateinc.com	US	1 (0.3%)
total active domains		271 (70.6%)

Table 5: Registrars of the 384 fast-flux domains as of May 7, 2008.

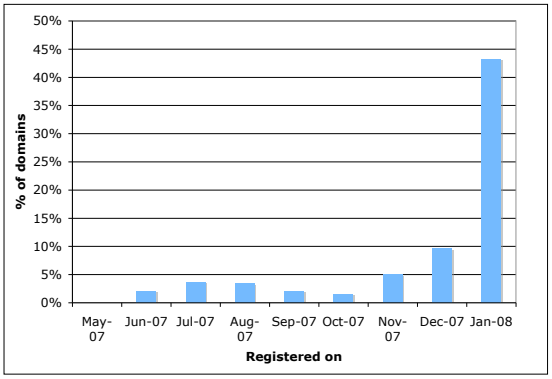


Figure 2: Record creation date for the 384 fast-flux domains: Y-axis is the percentage of the fast-flux domains that were registered on the particular month.

inactive domains as of May 2008 are due to registration expiration or some other reasons.

3.3 Limitations

Our data is derived from spam collected at a single spam trap; different spam traps might receive different distributions of spam emails from different locations. The relatively high volume of emails received at our spam trap (6,247,937 messages from the period of October 2007 through February 2008) suggests that the data we have collected may be representative of spam and scam campaigns seen at other networks, although our trap may certainly induce some geogprahic bias (for example, spam traps located in other countries may receive different scams). We sampled our dataset further by only actively monitoring a subset of the domains contained in URLs received in spam messages at the spam trap; in particular, we did not analyze domain names that we could not explicitly group into a scam campaign. Many of the domains that we could not group into a campaign also exhibited highly dynamic behavior, but we omitted these domains from the analysis because we could not confirm their participation in an online scam.

Unlike a legitimate site, a scam campaign operates under many different domain names (e.g., pathsouth.com, yesself.com), possibly to avoid URL blacklisting and perhaps to spread the risk of being detected and terminated by vigilant registrars. Our dataset may cover only a subset of these names for each campaign and we are unaware of any clear way to find out the true number of registered domain names for each scam campaign. However, in most cases, each do-

main within a campaign appears to show similar behavior.

In some cases, our DNS resolution process occurred months after the spam message corresponding to the scam was received at the spam trap. It is possible that the dynamics of fast-flux networks may differ close to the time of the receipt of the actual spam; however, our measurements suggest that the dynamics of fast-flux networks for each scam campaign (i.e., the rate of change of DNS records, the rate of accumulation of new IP addresses) remain stable over the course of a month, so it may be reasonable to expect similar dynamic behavior closer to the original receipt of the mail. We were surprised that most domains remained not only resolvable, but also reachable, even months after receipt of the original spam email associated with the campaign. This behavior differs from the dynamics of scam hosting sites observed in previous studies [2], which observed that many scam sites remain active for only a week; the difference may be due to the rise of fast-flux networks.

Our clustering technique assigns a URL to a *single* campaign based on snapshots of the Web site's content for a single snapshot. It is possible that, over time, a single domain could be used to host multiple campaigns; in these cases, our analysis would attribute behavior to a single campaign (i.e., the one corresponding to our snapshot) when, in fact, the domain was hosting multiple campaigns over the course of our analysis. We did not collect frequent enough snapshots to detect such behavior.

4. DYNAMICS

This section presents our findings concerning the dynamics of fast-flux service networks. We study three aspects of dynamics: (1) the rate at which DNS records change at each level of the hierarchy; (2) the rate at which fast flux networks accumulate new IP addresses (both overall, and by campaign); and (3) the location in the DNS hierarchy where dynamics are taking place. To understand the nature of these features with respect to "legitimate" load balancing behavior, we also analyze the same set of features for 500 popular sites listed by Alexa [1] as a baseline. We find many aspects of dynamics that are distinct to fast flux service networks.

4.1 Rate of Change

We studied the rates at which domains for online scams changed DNS record mappings and the corresponding TTL values for these records. We expected that fast-flux domains would both have short TTL values and exhibit frequent changes in name-to-IP address mappings.

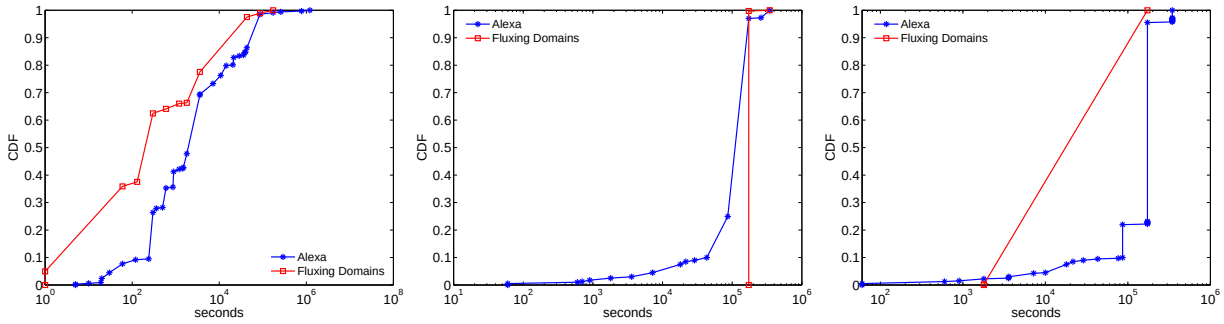
Figure 3 compares the distributions of TTLs between the fluxing domains and the domains in the Alexa data set. The disritubiotn of A record TTLs shows that scam sites have slightly shorter TTL values than popular Web sites; however, both classes of Web sites have A records with a wide range TTL values. Even more surprisingly, about 30% of popular Web sites maintain NS records with TTL values of less than a day, but almost all fast-flux domains we analyzed had TTL values for NS records of longer than a day. In hindsight, these results do make sense: many clients visiting scam sites will visit a particular domain infrequently, and only a small number of times, so the TTL value is less important than the rate at which the mapping itself is changing (i.e., for *new* clients that attempt to resolve the domain).

To detect changes that may be related to fast-flux behavior, we record both the A records that are returned at Step 6 in Figure 1, and NS names and IP addresses of NS names that are returned at Step 4. The reason why we record these two separate pieces of information is because NS names and IP addresses of NS names are not always returned with the A records of the answer at Step 6; the lack of complete information about the sequence of lookups in the DNS hierarchy will make it difficult to observe all aspects of the dynamics.

To account for possible load-balancing mechanisms at a higher level of the DNS hierarhcy, we group the responses according to the authoritative server that provided them. We then perform pairwise comparisons across each group of records. In the case of A records responses and NS record responses, we consider response as a change if at least one new record appears since last answer, or if the number of records returned has otherwise changed since the last response. (We do not consider reordering the records as a change.) In the case ofIP addresses of NS records, we consider the response to be a change if either NS names appear with different IPs or a new NS name shows up since last reply.

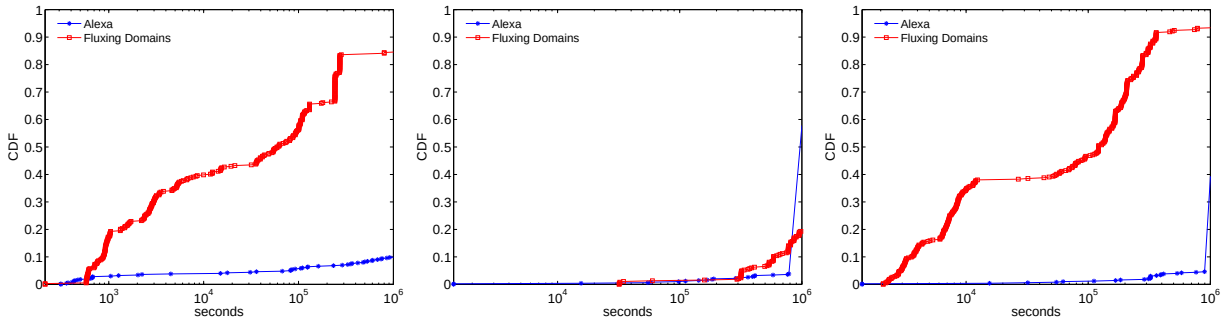
Fast-flux domains change on shorter time intervals than their TTL values. Figure 4 shows a distribution of the average time between changes for each domain across all 21 scam campaigns; each point on the line represents the average time between changes for a particular domain that we monitored. The distribution shows that fast-flux domains change hosting servers (A records) and name servers (IP addresses of NS records) more frequently than popular Web servers do. In particular, the rate of change of IP of NS records is much more frequent than TTL values of these records, causing possible service disruption for returning clients. In some cases, for example the IP addresses of NS records, the changes are significantly more frequent than the TTL values would suggest. The incongruence of DNS TTL values with the rates at which these records are actually changing could also prove to be a useful feature for detecting fast-flux behavior.

Domains in the same campaign tend to show similar rates of change. We also analyzed the rate of change of DNS records after clustering the fast-flux domains according to campaign. Figure 5 shows these results for the top 4 campaigns (ranked by the number of distinct IPs returned in A records for domains hosting the campaigns). The results are striking: different scam campaigns rotate DNS record mappings at distinct rates, and the rates at which DNS records for a particular campaign are remapped are similar across all domains for a particular scam. This finding suggests that it may be possible to use rates of flux at different levels in the



(a) A records (b) NS records (c) IP of NS records

Figure 3: Cumulative distribution of TTLs values of A, NS, and IP of NS records.



(a) A records (b) NS records (c) IP of NS records

Figure 4: Cumulative distribution of the average time between changes of A, NS, and IP of NS records.

DNS hierarchy as a type of signature for a scam campaign.

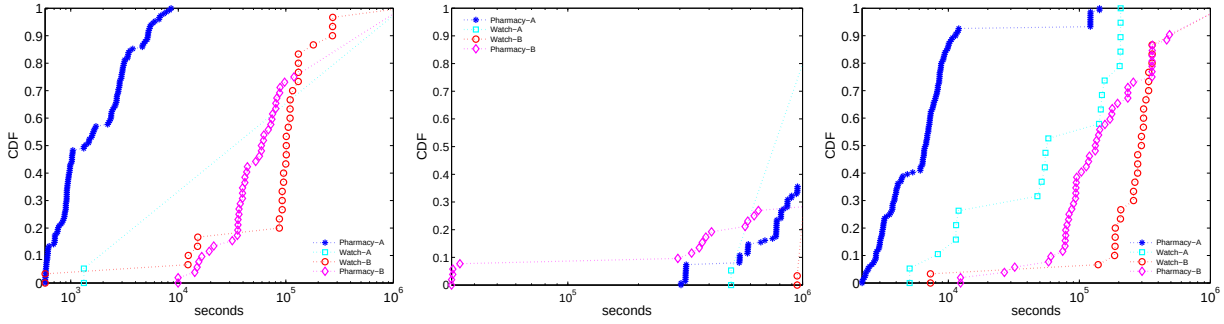
4.2 Rate of Accumulation

Ideally, we wish to know the size of a fast flux service network at a given moment and to measure the rate at which the network grows over time. However, in practice, our measurement is limited by the rate at which a flux domain updates its DNS records and what we present in this section is the rate at which a previously unseen host becomes an active hosting server (A records of a domain) or a name server (IP addresses of names returned by NS records).

Using a method similar to the one used by Holz *et al.* [6], we determine the rate of "flux" by repeatedly resolving each domain and assigning an increasing sequential ID to each previously unseen IP address. Figures 6(a) and 6(b) show the total number of distinct IPs for each fast-flux domain (the y-value of the end of each line) over the first week of our data collection period (first 2,000 iterations, 300 seconds apart from each other) and how fast each domain accumulated new hosts (slope). A steeper slope incidates more rapid accumulation of new IP addresses for that domain. Figure 6(a) shows this statistic for A records and Figure 6(b) shows the same statistic for IP addresses of NS records of the domains that belong to campaign Pharmacy-A (top campaign). Interestingly, the rate of accumulation is much slower (almost an order of magnitude) for hosts used as name servers, as shown in Figure 6(b).

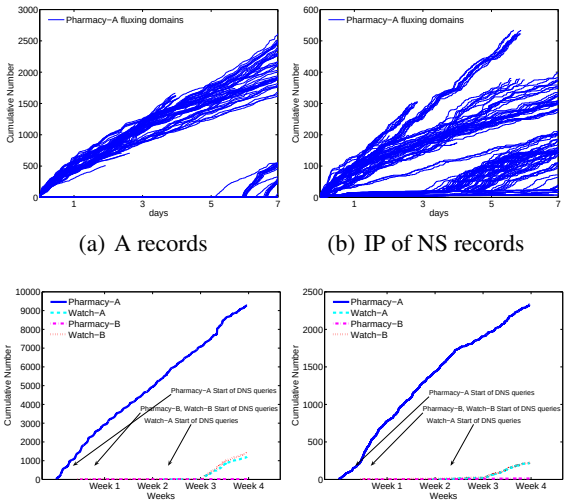
Many domains in the same campaign have similar accumulation rates. We see many domains with similar slopes throughout the month. These domains tend to belong to a same campaign. However, not all the fluxing domains belonging to the same campaign have similar slops (See Figure 6(c)). One reasonable explanation is that a scam campaign runs on multiple fast flux networks, each of which has a different rate of recruiting and swapping in a new host. In any case, it is alarming to see that many fluxing domains can easily throw in thousands of hosting servers and hundreds of name servers over a month.

Some domains only begin accumulating IP addresses after some period of dormancy. Some domains appear to exhaust available hosts for a while (days to weeks) before accumulating new IP addresses. We examined two campaigns that exhibited rapid accumulation of IP addresses after some dormancy. In both cases, only one domain per campaign begins accumulating IP addresses. These two domains shared exactly the same set of NS names. These 8 NS names are doing all the work for those two campaigns. We observed



(a) A records (b) NS records (c) IP of NS records

Figure 5: Cumulative distributions of the average time between changes of A, NS, and IP of NS records for Pharmacy-A, Watch-A, Watch-B, and Pharmacy-B.



(a) A records (b) IP of NS records

(c) A records - Top 4 (d) IP of NS records - Top 4

Figure 6: Cumulative number of distinct IPs for the A records and IP addresses of NS records, for the first week (first 2,000 iterations of data collection) for the Pharmacy-A domains, and for the top 4 campaigns across the four weeks of data collection.

Campaign	Fluxing domains	Location of change						
		A	[IP of NS]	NS	A+ [IP of NS]	A+ NS	NS+ [IP of NS]	A+NS +[IP of NS]
Pharmacy-A	149				77			72
Watch-A	30	4	1		24			1
Watch-B	19		18					1
Pharmacy-B	52	5	13		19			15
Casino-A	6		1		5			
Pharmacy-C	6		6					
Casino-B	1				1			
Links-A	2					1		1
Casino-C	5				5			
E-Marketing-A	4	4						
Pharmacy-D	50	2	3		45			
Pharmacy-E	4				4			
Links-B	35		1		34			
Pharmacy-F	2				2			
Pharmacy-G	2				1			1
Links-B	2			2				
Service-A	1				1			
Software-A	5		5					
Watch-C	5		4		1			
DomainNames-A	3	3						
Service-B	1			1				
Total	384	18	52	3	219	1		91
Alexa	500 (domains)	37	5	15	4	1	1	

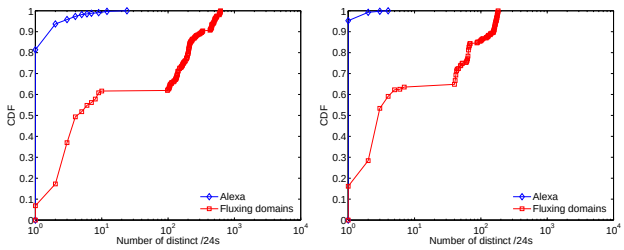
Table 6: Location of change for all campaigns, sorted by the total number of distinct IPs of A records.

other scams (e.g., the canadian pharmacy as well) where a few domains accumulate IP addresses faster than others. In addition to accumulation, we also saw attrition: 10% of fluxing domains became unreachable in the while we were monitoring them. These domains may have been blacklisted and so removed by registrars or by scamsters themselves.

Rates of accumulation differ across campaigns. Figures 6(c) and 6(d) show the rate of accumulation of IP addresses for the top four campaigns for the IP addresses of A records and NS records, respectively. The rate of accumulation for each campaign is higher than that of each fluxing domain. Because of resource sharing across the domains in a campaign, the total number of distinct IP addresses for a campaign is fewer than the sum of that of an individual domain. Section 5.2 will discuss how infrastructure is shared across domains and across campaigns in more detail.

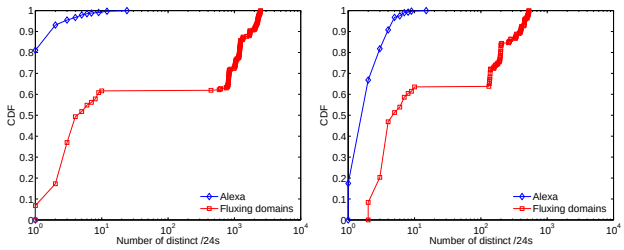
4.3 Location of Change in DNS hierarchy

While it is possible to change any record of your own domain in DNS hierarchy (A, NS, and IP addresses of NS records), it is substantially more difficult to change NS records or A records of name server names as this requires



(a) A records (b) IP of NS records

Figure 8: Distribution of unique /24s that appeared as the *first* record in a reply.



(a) A records (b) IP of NS records

Figure 9: Distribution of unique /24s that appeared for *all* records in a reply.

updating a parent domain's (often a top level domain such as .com) zone file. However, we see many fast-flux domains that freely change NS records or IP of NS records separately or in combination of other records.

Campaigns change DNS record mappings at different levels of the DNS hierarchy. Table 6 shows the type of change for each campaign. In contrast to previous studies [8, 21], we observe many different types of changes in addition to single flux (A records) and double flux (A + IP of NS). Another notable point is that each campaign tends to use mixes of techniques (e.g., For Pharmacy-A, 52% of domains are double flux and 48% change all three types of records). We believe that this is another indication that a campaign operates on multiple fast flux service networks.

5. ROLES

This section describes the roles (e.g., content hosting, name service, spamming) played by hosts in fast flux service networks and how these roles evolve over time. We first examine the geographic and topological locations of fast-flux nodes; we also compare these locations to the spamming hosts that mount the messages in the scam campagins. We then explore how the roles of fast-flux nodes evolve over time, and how the fast-flux infrastructure is shared across different scam campaigns.

5.1 Location

In this section, we examine the network and geographic location of fast flux hosts and compare them to both legitimate Web sites and the spammers who advertise the scams.

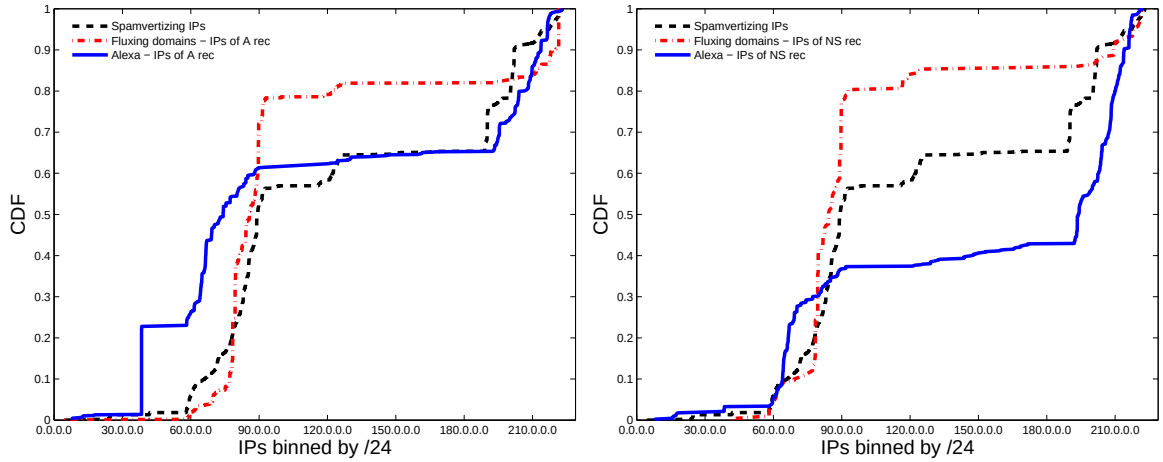
5.1.1 Network Location

This section describes how fast-flux IP addressess are spread across IP address space. To examime whether fast-flux service networks use different portions of the IP space than the top 500 domains, we plotted the distribution of the IPs across the whole IP range. Figure 7 shows that fast-flux networks use a different portion of the IP space than sites that host popular legitimate content: The IPs that host legitimate sites are considerably more distributed: and more than 30% of these sites are hosted in the 30/8-60/8 IP address range, which hosted almost none of the scam sites observed in our study.

Fast-flux hosts are concentrated in small regions of IP address space; some spammers are concentrated in slightly different regions. Interestingly, the IP address space that hosts fast-flux domains is even more concentrated than that which sends spam advertising the scam campaigns. Although the distributions are ismilarly concentrated in the 80/8 - 90/8 range, there is a much higher concentration of spammers in the 200/8 - 210/8 range (ranges allocated to Latin America and Asia, respectively). These differing distributions suggest that hosts in different regions of the IP address space do in fact play different "roles" in spam campaigns.

DNS lookups for fast-flux domains often return much more widely distributed IP addresses than lookups for legitimate Web sites. Our intuition was that fast-flux networks that hosted scame sites would be more distributed across the network than legitimate Web hosting sites, particularly from the perspective of DNS queries from a single client (even in the case of a distributed content distribution network, DNS queries would tend to map a single client to nearby Web cache). Figures 8 and 9 show the distribution of distinct /24s that appear at the answer section of the DNS replies) for the first record in the reply and for all records in the reply, respectively. It turns out that a few legitimate domains that are hosted by content distribution networks appear to have the largest number of distinct /24s contained in a single DNS reply. In particular, `www.runescape.com`, `www.statcounter.com`, `www.yahoo.co.jp`, `www.monografias.com` returns IP addresses in 12, 8, 7, and 6 distinct /24s respectively. We also observed several legitimate domains which showed a large number of distinct /24s for their IPs of NS records (which actually reflects good network design because it introduces redundancy). Examples include `www.altavista.com`, `www.geocities.com`, `www.runescape.com`, `www.php.net` which had 11, 9, 8, and 7 distinct /24s in IPs of NS records.

Fast flux domains tend to return IP addresses that are distributed across a larger number of distinct /24s than le-



(a) A records (b) IP of NS records

Figure 7: Distribution of the IPs of A rec, of autoritative servers and the IPs that sent the originating spam.

Top ASes by A Rec	Top ASes by IP of NS Rec	Top ASes by Spamming IPs
8402 - CORBINA-AS (1232)	12714 TI-AS NetByNet Holding (365)	9121 TTNET (6566)
12714 - TI-AS NetByNet Holding (1127)	3904 - HUTCHISON-AS-AP (260)	6147 Telefonica del Peru (3173)
9304 - HUTCHISON-AS-AP (951)	8402 - CORBINA-AS (224)	22927 Telefonica de Argentina (2726)
7132 - AT& T (511)	7132 - AT& T (121)	5617 TPNET Polish Telecom (2356)
6855 - SK SLOVAK TELECOM (345)	9908 - HKCABLE2-HK-AP (91)	19262 VZGNI-TRANSIT Verizon (2107)
13184 - HANSENET (332)	12695 - DINET-AS (81)	4837 CHINA169-BACKBONE (1697)
12695 - DINET-AS (307)	20597 - ELTEL-AS (72)	7738 Telecomunicacoes da Bahia (1524)
3209 - Arcor IP-Network (270)	13184 - HANSENET(66)	8359 COMSTAR (1436)
8615 - CNT-AS (252)	4766 - KIXS-AS-KR Korea Tel. (60)	4134 CHINANET-BACKBONE (1344)
3320 - DTAG (203)	30784 - ISKRATELECOM-AS(59)	9829 BSNL-NIB (1340)

Table 7: Top 10 ASes by number of IPs.

gitimate domains. Indeed, roughly 40% of all A records returned for fast-flux domains were distributed across at least 300 distinct /24s, and many were distributed across thousands of /24s. In contrast, domains for popular Web sites were never distributed across more than 12 distinct /24s (when queried from a single location). Thus, overly widespread distribution of query replies may serve as a strong indicator that a domain is indeed hosted by a fast-flux network.

The predominant networks that host fast-flux infrastructure differ from those that host spammers for the corresponding scam campaigns. Table 7 shows the top ten ASes by the number of IP addresses for A records (i.e., hosting sites), NS records (i.e., nameservers), and spammers (as observed in the spam trap). Interestingly, although there is some overlap between the ASes that host the scam sites and those that host authoritative nameservers, there is almost no overlap between the ASes that host the sites and nameservers for the scams do not overlap much with the ASes hosting the spamming IP addresses. Indeed, Figure 7 also shows that spammers for the campaigns we observed are more heavily concentrated in Latin America, Turkey, and the United States, whereas fast-flux hosts are more concentrated in Asia. The fact that significant differences exist between networks that host fast-flux infrastructure and those that host spammers suggest that scammers may have divided the infrastructure into different roles (in Section 6, we see that many fast-flux hosts are not listed on spam blacklists, which is consistent with this observation).

5.1.2 Geographic location

Hosting servers and name servers are widely distributed. Table 8 lists country names in which fast flux nodes are hosted, according to the country of the AS in which they are hosted. In total, we observed IP addresses for A records in 283 ASes across 50 countries, IP addresses for NS records in 191 ASes across 40 countries, and IP addresses for spammers for the corresponding scam campaigns across 2,976 IP addresses across 157 countries. Although many fast flux nodes appear to be in Russia, Germany, and the US, the long list of ASes and countries shows that fast flux service networks are truly distributed; this kind of geographical distribution may be necessary to accommodate the diurnal pattern of compromised hosts' uptime [5]. Interestingly, the countries that are referred to by the most A records are not the same set of countries that host authoritative nameservers for

Top Countries by A Rec	Top Countries by IP of NS Rec	Top Countries by Spamvertising IPs
Russia (4025)	Russia (982)	US (6972)
Germany (1207)	Hong Kong (425)	Turkey (6580)
Hong Kong (1207)	Germany (216)	Russia (5914)
US (606)	US (168)	Brazil (4606)
Slovakia (391)	Korea (154)	Argentina (4268)
Korea (350)	China (77)	China (4041)
Israel (337)	Japan (64)	Poland (3424)
Japan (248)	Taiwan (48)	India (3302)
Ukraine (247)	Ukraine (40)	Peru (3214)
Romania (131)	Slovakia (39)	Germany (3122)

Table 8: Top 10 countries by number of IPs.

Sharing of A records				
	Pharmacy-A	Watch-A	Watch-B	Pharmacy-B
Total per campaign	9448	1516	1204	15
Pharmacy-A	-	1510	1203	1
Watch-A	1510	-	1203	1
Watch-B	1203	1203	-	1
Pharmacy-B	1	1	1	-
Sharing of NS records				
	Pharmacy-A	Watch-A	Watch-B	Pharmacy-B
Total per campaign	52	14	10	10
Pharmacy-A	-	8	8	0
Watch-A	8	-	8	0
Watch-B	8	8	-	0
Pharmacy-B	0	0	0	-
Sharing of IPs of NS records				
	Pharmacy-A	Watch-A	Watch-B	Pharmacy-B
Total per campaign	2340	225	219	13
Pharmacy-A	-	220	215	9
Watch-A	220	-	215	9
Watch-B	215	215	-	6
Pharmacy-B	9	9	6	-

Table 9: Sharing among the top 4 campaigns.

those domains (as indicated by IP addresses of NS records). In particular, Slovakia, Israel, and Romania appear to host relatively more nameservers than sites, and China appears to host relatively more nameservers. This difference in distribution deserves further study; one possible explanation is that nameserver infrastructure for fast-flux networks must be more robust than the sites that host scams (which might be relatively transient). countries

5.2 Sharing Across Campaigns

In this section, we describe our findings regarding the sharing of the same fast-flux infrastructure across multiple scam campaigns.

Many fast-flux machines have dual roles, and different campaigns share hosting infrastructure. Referring back to Table 3, the last three columns indicate that many hosting servers double as name servers (and vice versa). 16 out of 21 campaigns (76%) show such sharing. On the contrary, we see a clear role separation of the hosts associated with the domains of the popular Web sites listed by Alexa. We also find significant overlaps among the hosts involved for the top four campaigns. Table 9 shows that Watch-A and Watch-B are likely to share the underlying infrastructure—99% of hosting servers, 80% of NS records, and 98% of name servers of Watch-B are common with those used for Watch-A. Moreover, both campaigns share many of the servers and NS records with Pharmacy-A. This overlap strongly suggests that the all three campaigns involve same fast-flux service networks. Interestingly, our observation is consistent with Spam Trackers [14], which attributes all the three scam campaigns to Yambo Financials [15].

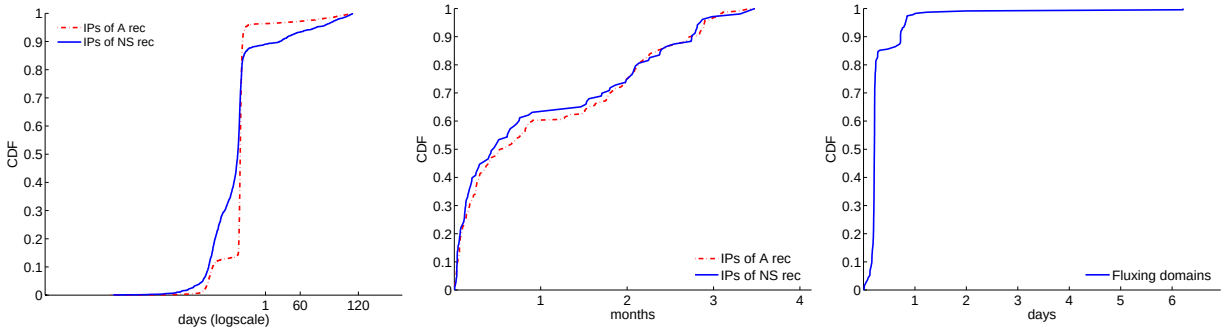
6. RELATIONSHIP TO BLACKLISTS

In this section, we evaluate whether the IPs that show up as part of the fast-flux network hosting infrastructure appear on various blacklists: (1) the Spamhaus spam blacklist (SBL/PBL) [19]; (2) the Spamhaus exploit blacklist (XBL) [20]; and (3) the URI blacklist (URIBL) [22]. We find, generally, that the time to blacklisting varies significantly by blacklist, and that many fast-flux IP addresses are not listed in the SBL; those that are tend to be listed both before and after we observed fast-flux activity.

Method. To determine whether the IP addresses in our dataset are blacklisted at the time that we witness them as part of fast-flux infrastructure, or whether they become blacklisted at some later point, we query each blacklists database for historical information about listing. Georgia Tech actively runs mirrors for SpamHaus SBL/PBL/XBL and for URIBL, which gives us access to precise information about when each IP address or domain is listed in the database. We query the following databases:

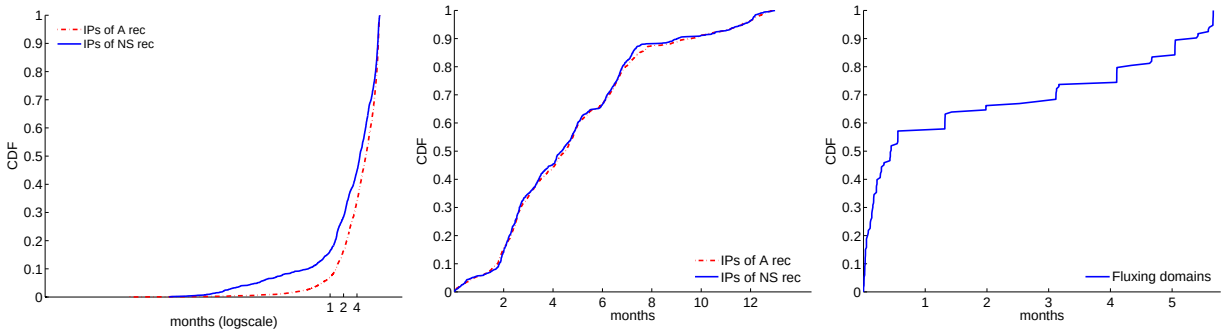
- XBL, a real-time database of IP addresses of infected machines including open proxies worms/viruses with built-in spam engines, and other types exploits.
- SBL, a realtime database of IP addresses of verified spam sources and spam operations.
- PBL, a database of end-user IP address ranges that should not be delivering unauthenticated SMTP email to any Internet mail server except those provided for specifically by an ISP for that customer's use.
- URIBL, a realtime blacklist that lists domains that appear in spam and are likely phishing or scam sites.

Many fast-flux IP addresses and domains do not appear in blacklists at the time when their activity is first observed. We queried the blacklist data at the end of April 2008 for historical information (back to February 2007) for each IP address and domain from our dataset. Table 10 shows the number of IPs that were already blacklisted before we observed them at our dataset, IPs that were blacklisted after we observed them in our dataset, IPs that were blacklisted as active before and after we observed, and finally IPs that were never blacklisted (by the time we querried the BLs database). Table 10 shows that a significant fraction of IP addresses hosting scam infrastructure (more than 17%) were never listed in the SBL; considerably higher fractions were listed in the XBL and URIBL, although many of the IP ad-



(a) XBL (b) SBL/PBL (c) URIBL

Figure 10: CDF of time elapsed between the appearance of an IP address in our dataset, either as IP of A record or IP of NS record of a fluxing domain and the timestamp of appearance at Spamhaus BL. Also the same for the fluxing domains and the elapsed time before they were blacklisted at URIBL.



(a) XBL (b) SBL/PBL (c) URIBL

Figure 11: CDF of time elapsed between the appearance of an IP address, either as IP of A record or IP of NS record of a fluxing domain at a blacklist, and the timestamp of appearance in our dataset (The "opposite" from Figure 10).)

	SBL/PBL				XBL				
	Never	B	A	B+A	Never	B	A	B+A	Total
A	1692	29	283	7517	265	244	2648	6364	9521
NS	547	7	80	1787	183	98	481	1659	2421

	URIBL				
	Never	B	A	B+A	Total
Domains	113	0	138	133	384

Table 10: IPs of A records, IPs of NS records and domains which were blacklisted before (B), after (A) or before and after (B+A) when they appeared at our collection of DNS records.

dresses and domains listed in the XBL and URIBL respectively were only listed *after* we observed activity from those IP addresses and domains. The lack of these IP addresses in the SBL could suggest one of two things: (1) the SpamHaus SBL is incomplete; or (2) the SBL may simply not list this fraction of IP addresses because it was never used to spam (i.e., it only hosted scam infrastructure).

Time to listing after activity is observed can vary from hours to weeks, depending on the blacklist. IP addresses tend to take longer to show up in the Spamhaus SBL. To determine how long it takes for IP addresses to appear in various blacklists after we observed their activity, we measured the time between when we observed the IP addresses participating in fast-flux activity and the time when they were first blacklisted. Figure 10 shows the distribution of these delays. We plot the CDFs of the elapsed times between appearance and listing for XBL, SBL/PBL, and URIBL.

Most IP addresses are listed relatively quickly (if they are not already listed when we observe either activity), but for some IP addresses and domains, the time that elapses between the time we first observe activity and the time an IP address or domain is listed is on the order of weeks. These delays in listing IP addresses in the SBL suggests that there are parts of fast-flux networks that are used first as flux agents and later as spam relays. In these cases, monitoring hosts for fast-flux activity may be useful for predicting future spamming activity. Figure 11 shows the same distri-

	Not appeared	Before	After	Bef.+After	Total
IPs of A rec	9417	11	92	1	9521
IPs of NS rec	2420	5	16	0	2421

Table 11: IPs of A records, IPs of NS records and domains which appeared at our spamtrap as spam relays before (B), after (A) or before and after (B+A) their time of appearance at our collection of DNS records.

bution, but for IP addresses that were listed before we observed activity from them in our dataset. Interestingly, most IP addresses that were listed before we observed their activity were listed in the XBL weeks to months before we observed them (IP addresses for A records were listed sooner).

We observe a small amount of overlap between IP address that host fast-flux infrastructure and those that send spam to our spam trap. To further understand the relationship between spamming infrastructure and the scam hosting infrastructure, we examined the overlap between IP addresses that spam and those that host infrastructure: For each IP address that we observed (IPs of A records and IPs of NS records), we checked to see whether the IP had sent any spam emails to the same spam trap from which we extracted the fluxing domains over the period of October 2007 through February 2008 (i.e., from nearly three months before the start of our collection of fast flux data until 1 month after our data collection). Table 11 shows that a very small fraction of IP addresses (about 1%) sent spam to our spam trap either before or after the time when we observed them as part of the scam hosting infrastructure. The small overlap may simply reflect the fact that our trap only sees a fraction of all spam (and spammers). These spamming IPs advertise the same fast-flux domains that they are hosting, which suggests that the spamming infrastructure and the hosting infrastructure may be shared.

7. CONCLUSION

This paper has presented an empirical study of the dynamics and roles of fast-flux networks in mounting scam campaigns. We actively monitored the DNS records for URLs for scam campaigns received at a large spam sinkhole over a one-month period to study the rates of change in fast-flux networks, the locations in the DNS hierarchy that change, and the extent to which the fast-flux network infrastructure is shared across different campaigns. We also contrast the dynamics observed in these networks to that used for load balancing for popular Web sites. Our findings suggest that monitoring the infrastructure for unusual changes in DNS mappings may be helpful for detecting scams hosted on fast-flux networks. In future work, we plan to use these features design a detection scheme that can automatically identify scam campaigns based on invariant properties of the infrastructure. We expect that doing so may allow us to detect online scams automatically, and considerably faster than today's manual blacklisting mechanisms.

REFERENCES

[1] Alexa. Alexa the Web Information Company. http://www.alexa.com/, 2008.

[2] D. S. Anderson, C. Fleizach, S. Savage, and G. M. Voelker. Spamscatter: Characterizing Internet Scam Hosting Infrastructure. In *USENIX Security Symposium*, Aug. 2007.

[3] http://www.autoitscript.com/autoit3/.

[4] D. Dagon, C. Zou, and W. Lee. Modeling Botnet Propagation Using Time Zones. In *The 13th Annual Network and Distributed System Security Symposium (NDSS 2006)*, San Diego, CA, Feb. 2006.

[5] D. Dagon, C. Zou, and W. Lee. Modeling Botnet Propagation Using Time Zones. In *NDSS*, Feb. 2006.

[6] T. Holz, C. Corecki, K. Rieck, and F. C. Freiling. Measuring and Detecting Fast-Flux Service Networks. In *NDSS*, Feb. 2008.

[7] ICANN. ICANN-Accredited Registrars. http://www.icann.org/registrars/accredited-list.html, 2008.

[8] ICANN Security and Stability Advisory Committee. SSAC Advisory on Fast Flux Hosting and DNS. http://www.icann.org/committees/security/sac025.pdf, Mar. 2008.

[9] IEInspector Software LLC. IEInspector HTTP Analyzer — HTTP Sniffer, HTTP Monitor, HTTP Trace, HTTP Debug. http://www.ieinspector.com/httpanalyzer/, 2007.

[10] J. Jung and E. Sit. An Empirical Study of Spam Traffic and the Use of DNS Black Lists. In *Internet Measurement Conference*, Taormina, Italy, October 2004.

[11] A. Pathak, Y. C. Hu, and Z. M. Mao. Peeking into Spammer Behavior from a Unique Vantage Point. In *First USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET)*, San Francisco, CA, Apr. 2008.

[12] M. Rajab, J. Zarfoss, F. Monrose, and A. Terzis. A Multifaceted Approach to Understanding the Botnet Phenomenon. In *ACM SIGCOMM/USENIX Internet Measurement Conference*, Brazil, Oct. 2006.

[13] A. Ramachandran and N. Feamster. Understanding the Network-Level Behavior of Spammers. In *SIGCOMM*, Sept. 2006.

[14] Spam Trackers. Fast-flux. http://spamtrackers.eu/wiki/index.php?title=Fast-flux, Oct. 2007.

[15] Spam Trackers. Category:Yambo family. http://spamtrackers.eu/wiki/index.php?title=Category:Yambo_family, Mar. 2008.

[16] Spam Trackers. Diamond Replicas. http://spamtrackers.eu/wiki/index.php?title=Diamond_Replicas, Apr. 2008.

[17] Spam Trackers. Exquisite Replica. http://spamtrackers.eu/wiki/index.php?title=ExquisiteReplica, Mar. 2008.

[18] Spam Trackers. Canadian Pharmacy. http://spamtrackers.eu/wiki/index.php?title=Canadian_Pharmacy, Apr. 2009.

[19] Spamhaus SBL. http://www.spamhaus.org/sbl.

[20] Spamhaus XBL. http://www.spamhaus.org/xbl.

[21] The Honeynet Project. Know Your Enemy: Fast-Flux Service Networks. http://www.honeynet.org/papers/ff/, July 2007.

[22] URIBL. http://www.uribl.org/.

[23] Y. Xie, F. Yu, K. Achan, E. Gillum, M. Goldszmidt, and T. Wobber. A Multifaceted Approach to Understanding the Botnet Phenomenon. In *ACM SIGCOMM*, Kyoto, Japan, Aug. 2007.

[24] B. Zdrnja, N. Brownlee, and D. Wessels. Passive Monitoring of DNS Anomalies. In *DIMVA*, July 2007.